# Investigating privacy in an ambient world

**Linda Little**
PACT Lab
School of Psychology and Sports Science
Northumbria University, UK
+44 191 2437250
l.little@northumbria.ac.uk

**Pam Briggs**
PACT Lab
School of Psychology and Sports Science
Northumbria University, UK
+44 191 2274570
p.briggs@northumbria.ac.uk

**ABSTRACT**
Ambient Intelligence (AmI) and ubiquitous computing allow us to consider a future where computation is embedded into our daily social lives. This vision raises its own important questions and augments the need to understand how people will achieve and maintain privacy. As a result, we have recently conducted a wide reaching study of people's attitudes to potential AmI scenarios with a view to eliciting their privacy concerns. The focus of this paper will be on the method used and preliminary findings will be discussed.

**Keywords**
Privacy, ambient technology, scenarios

**INTRODUCTION**
Ambient Intelligence (AmI) refers to the convergence of ubiquitous computing, ubiquitous communication, and interfaces that are both socially aware and capable of adapting to the needs and preferences of the user. AmI evokes, or perhaps presages, a near future in which humans will be surrounded by 'always-on', unobtrusive, interconnected intelligent objects, few of which will bear any resemblance to the computing devices of today. Devices embedded in the environment will communicate seamlessly about any number of different topics, e.g., your present state of health, when you last ate, and what it was you ate. Interactions with other devices, and at the same time other people, will become anywhere, anytime.

The majority of current work on AmI is driven by technological considerations, despite claims that it is fundamentally a human-centred development that will essentially set people free from the desktop. One of the particular challenges of AmI is that the user will be involved in huge numbers of moment-to-moment exchanges of personal data without explicitly sanctioning each transaction.

In the present we already carry around devices (e.g. mobile phones, personal digital assistants) that exchange personal information with other devices – but we initiate most exchanges ourselves. The seamless exchange of information has vast social implications and in particular pushes privacy concerns to the forefront.

**Privacy**
Every major advance in information and communication technologies since the late 19th century has increased concern about individual privacy [11]. AmI brings new and increased risks, including fraud and identity theft, and therefore we see privacy control as essential in AmI.

There is no universal definition of privacy, the concept is highly complex and involves different perspectives and dimensions. The need and desire for privacy varies between individuals, cultures, social and physical environmental factors. The desired level of privacy relates to what an individual wants and the achieved level is what they actually obtain. We need to understand how privacy is achieved and maintained in both physical and virtual worlds.

**Privacy in the virtual world**
Future systems will enable more freedom and reduce the physical constraints of time and place. Development in technology is considered to be the main culprit responsible for increasing concern over the protection of privacy. We already know that perceptions of privacy impact upon current technology use [6]. As new forms of technology are introduced, personal information may be accessed using a variety of different systems.

In an ambient world information collection, processing and sharing are fundamental procedures needed for the systems to be fully aware of the user's needs and desires [4]. AmI technologies will act on the user's behalf without their explicit knowledge and the interaction will be invisible. By its very nature this puts ambient technology and privacy in conflict. We need to understand this conflict and how privacy impacts upon AmI technology adoption and use.

Although several programs exist to stop personal details being collected, individuals may not know how to install or

use them. Privacy preference protocols and systems such as P3P allow users to set preferences in accordance with their privacy needs. However, we must question whether this concept would truly work in an AmI society. Palen & Dourish [10] argue that as our lives are not predictable, and privacy management is a dynamic response to both the situation and circumstance, prior configuration and static rules will not work. Therefore, disclosure of information needs to be controlled dynamically. Olsen et al [9] take an opposite view and suggest individuals can set preferences for sharing information as people tend to have clusters of similar others and therefore the task is not as complex or particularly difficult to undertake as it first may seem.

Academics, researchers and industry acknowledge that AmI technologies introduce a new privacy risk [11]. Privacy control in an AmI world is essential to decrease risks such as fraud and identity theft. Consider the following question: Will users be able to set their own privacy preferences? The answer seems easy, but is it? Humans live, work and interact with a variety of people and in different environments. The multifaceted nature of human-human interaction requires each individual to set complex sets of privacy preferences dependent upon their situation and circumstance. These preferences would also have to remain stable across place, space, country and culture.

If AmI technologies are used globally, systems must be designed so that user privacy settings remain secure and unchanged across international boundaries. For example, Europe has a tighter data protection act compared to the USA [3]. Therefore someone travelling from Europe to the USA might find unknown others have access to his or her personal information when entering the country due to the slacker regulation and control of privacy policies related to AmI systems.

**Privacy in the physical world**

When considering human interaction with technology in any context, privacy is a very important issue. In the future individuals will be able to use systems in a multitude of different social environments and be interacting with a variety of people, whether friends, family or complete strangers.

Concerns already exist about certain technologies used in public places e.g. surveillance cameras. People have been 'watched' and their behaviour recorded in public places for many years. Many arguments exist for the use of such cameras, e.g. crime reduction. However as advances in surveillance technologies are made many now argue that privacy no longer exists, or that if it does it is quickly disappearing as our activities are increasingly made public [1].

Another area of growing concern for users of technology is tracking. Users of mobile telephones are already aware their service provider can track their location. However design specifications in future technologies may mean it is not only the service provider who knows where you are and what you are doing. The future could see systems developed that track users to specific locations whether their device is switched on or off. Tracking will not only be available to the service provider but to virtually anyone who wants to know where the user is. Although this may be a good idea, for example in the case of missing persons, it does raise important ethical issues.

A recent study [2] found individuals are willing to disclose something about their location most of the time. However, the individual will only disclose information when: the information is useful to the person requesting it, the request is timely, is dependent upon the relationship he or she has with the requestor and why the requestor needs the information. These findings highlight the need for control and choice over disclosure of personal information at any one point in time.

**Problems with privacy**

Problems exist when trying to understand and investigate privacy issues when related to both physical and virtual worlds. No one theory or approach is sufficient to explore this complex topic.

Findings from privacy research in the Human Computer Interaction (HCI) and computer science areas tend to focus on security aspects of existing or hypothetical systems. However recent studies are now acknowledging the complex nature of human-human interaction and the need for users to set multiple privacy preferences in an AmI world [11].

Concerns have also been raised in privacy research due to the actual concept itself, i.e. individuals both protect and manage it. Levels of control and actual context of the interaction all have a major affect on use of AmI technology and the user. We need to understand how people will regulate, control and choose when to interact with such devices and who will have access to their personal information.

To fully understand privacy we need to consider: how humans interact with each other, how humans interact with technology, how technologies communicate with other technologies and know the technical constraints of each system. The aim of this research is to investigate how people will control information exchange when using AmI devices by focusing on the concept of privacy.

**Method**

To understand and investigate the concept of AmI technology and subsequent use key stakeholders provided specific scenarios illustrating the ways in which privacy, trust and identity information might be exchanged in the future. The stakeholders included relevant user groups, researchers, developers, businesses and government departments with an interest in AmI development. Four scenarios were developed, related to health, e-voting, shopping and finance that included facts about the device, context of use, type of service or information the system would be used for.

The elicited scenarios were scripted and the scenes were videotaped in context to develop Videotaped Activity Scenarios (VASc). The VASc method is an exciting new tool for generating richly detailed and tightly focussed group discussion and has been shown to be very effective in the elicitation of social rules [7]. VASc are developed from either in-depth interviews or scenarios, these are then acted out in context and videotaped. The VASc method allows individuals to discuss their own experiences, express their beliefs and expectations. This generates descriptions that are rich in detail and focussed on the topic of interest. For this research a media production company based in the UK was employed to recruit actors and videotape all scenarios. The production was overseen by both the producer and the research team to ensure correct interpretation. British Sign Language (BSL) and subtitles were also added to a master copy of the VASc's for use in groups where participants had various visual or auditory impairments.

**Participants**

The VASc's were shown to thirty-eight focus groups, the number of participants in each group ranged from four to twelve people (N=304). Participants were drawn from all sectors of society in the Newcastle upon Tyne area of the UK, including representative groups from the elderly, the disabled and from different ethnic sectors. Demographic characteristics of all participants were recorded related to: age, gender, disability (if any), level of educational achievement, ethnicity, and technical stance. As this study was related to future technology it was considered important to classify participants as either technical or non-technical. This was used to investigate any differences that might occur due to existing knowledge of technological systems. Therefore participants were allocated to groups initially by technical classification i.e. technical/non-technical, followed by gender, then level of educational achievement (high = university education or above versus low = college education or below), and finally age (young, middle, old).

**Procedure**

On recruitment all participants received an information sheet that explained the study and the concept of AmI technologies. Participants were invited to attend Northumbria University, UK to take part in a group session. The groups were ran at various times and days over a three-month period. Participants were told they would be asked to watch four short videotaped scenarios showing people using AmI systems and contribute to informal discussions on privacy and trust permissions for this type of technology. They were told all of the other participants in their particular group would be of approximately the same age and gender and informed the discussion groups would be recorded for further analysis.

At the beginning of each group session the moderator gave an explanation and description of AmI technologies. After the initial introduction the first videotaped scenario was shown. Immediately after this each group was asked if they thought there were any issues or problems they could envisage if they were using that system. The same procedure was used for the other three-videotaped scenarios. The scenarios were viewed by all groups in the same order: e-voting, shopping, health and finance. Once all the videos had been viewed an overall discussion took place related to any advantage/disadvantages, issues or problems participants considered relevant to information exchange in an ambient society. Participant's attitudes in general towards AmI systems were also noted.

**Results**

All group discussions were transcribed then read; a sentence-by-sentence analysis was employed. The data was then open coded using qualitative techniques and several categories were identified. The data was physically grouped into categories using sentences and phrases from the transcripts. Categories were then grouped into the different concepts, themes and ideas that emerged during the analysis.

The various themes and concepts that emerged from the analysis provided greater insight into privacy issues regarding information exchange in an ambient society. The main constructs related to privacy regulation and control were:

a) *Physical*: how physically accessible a person is to others
b) *Informational*: a person's right to reveal personal information to others.
c) *Social*: the ability to control social interactions between social actors.
d) *Psychological*: a person's right to decide with whom they share personal information.
e) *Choice*: the right to choose
f) *Control*: the right to control
g) *Security*: security aspects related to transmission and storage of information.

**Discussion**

The findings from this research support the view privacy is a multidimensional construct with underlying factors that

dynamically change according to context. When interacting with technology privacy protection and disclosure of information is a two-way process.

To establish privacy the following questions need to be addressed when related to information exchange: Who is receiving it? Who has access? Is the receiver credible, and predictable? Where is the information being sent and received? Does the user have choice and control? How does the device know who to communicate with, e.g. through personalised agents? This raises interesting questions regarding permission setting within an AmI context – regarding the extent to which individuals should be allowed to make day to day decisions about who or what to trust on an ad hoc basis, or should employ agent technologies that represent their personal trust and privacy preferences and communicate these to other agents [8].

Disclosure of information in any form or society is a two-way process. Findings support, the Fair Information Practice-FIP (e.g. Federal Trade Commission of America 2000) that suggests companies should give users: notice, choice, access and security. We need to consider the following guidelines when considering adoption and use of AmI systems:

a) Choice: the option to reveal or hide information
b) Control: the ability to manage, organise and have power over all information exchanged and to notified of information held about you
c) Transparency: the need for stakeholder's to be open to information held about a person and for that person to have a right to access and change such information
d) Global rules and regulations: a global infrastructure of rules related to information exchange
e) Obscurity: the need for information exchange to be closed or made ambiguous dependent on the user's needs and desires at anyone moment in time
f) Trust and privacy preference: the need for the user to set preferences that can be dynamic, temporary and secure.

These guidelines are basic and we need to consider the fact humans are inherently social beings and their actions are always directly or indirectly linked to other people. Practices such as FIP are needed to mediate privacy, empower the individual, increase the users control and create assurance. These policies also reduce data-gathering, data-exchanging and data-mining and therefore important in an ambient society.

The method used in this research has proved very successful in trying to understand privacy in an ambient society. Further experimental work will be undertaken to validate these findings.

**References**


1. Bin, D. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*. England: Perseus Press (1998).
2. Consolvo, S. ,. Smith, I.E. Matthews, T. , LaMarca , A., Tabert, J., & Powledge, P. Location disclosure to social relations: why, when, & what people want to share, Proceedings of the SIGCHI conference on Human factors in computing systems, April ,Portland, Oregon, USA (2005)
3. Dawson, L., Minocha, S., & Petre, M. *Social and Cultural Obstacles to the (B2C) E-Commerce Experience.* Paper presented at the People and Computers XVII - Designing for Society, (2003).,25-241
4. Dritsas, S., Gritzalis, D., & Lambrinoudakis, C. Protecting privacy and anonymity in pervasive computing trends and perspectives. *Telematics and Information*. (2005) In Press
5. FTC Study Privacy Online: Fair Information Practices in the Electronic Marketplace . A Report to Congress, May. (2000)
6. Little, L., Briggs, P., & Coventry, L. Public Space Systems: Designing for privacy? *International Journal of Human Computer Studies*.63, (2005). 254-268
7. Little, L., Briggs, P., & Coventry, L.. Videotaped Activity Scenarios and the Elicitation of Social Rules for Public Interactions. BHCIG Conference, Leeds, September 2004
8. Marsh, S.,. *Formalising Trust as a Computational Concept.* PhD Thesis, University of Stirling, Scotland.(1994) Available online via www.stephenmarsh.ca
9. Olsen, K., Grudin, J., Horvitz, E. 'A study of preferences for sharing and privacy'. *CHI, 2005 extended abstracts on Human factors in computing systems*
10. Palen, L. & Dourish, P.. Unpacking Privacy for a Networked World. *Proceedings of the ACM, CHI (2003),5 (1), 129- 135.*
11. Price, B. A., Adam, K., & Nuseibeh, B. Keeping Ubiquitous Computing to Yourself: a practical model for user control of privacy. *International Journal of Human-Computer Studies, 63,(2005) 228-253*